(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 110012496 A
(43)申请公布日 2019.07.12

(21)申请号 201910340934.2

(22)申请日 2019.04.25

(71)申请人 江苏创通电子股份有限公司
地址 215300 江苏省苏州市昆山经济技术开发区雄鹰路178号3号楼1楼

(72)发明人 肖炼斌 叶丁 周永贵 鲍雪刚 张胜利 杨磊

(74)专利代理机构 北京路浩知识产权代理有限公司 11002
代理人 王庆龙 苗晓静

(51)Int.Cl.
H04W 24/08(2009.01)

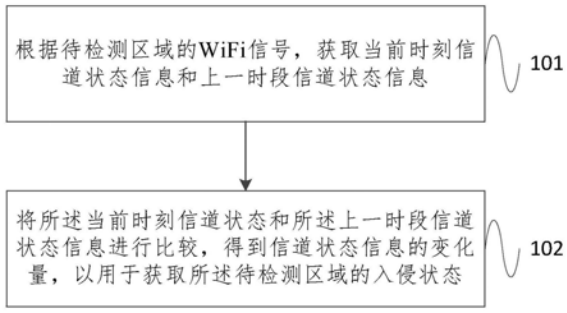
权利要求书2页 说明书7页 附图1页

(54)发明名称

一种基于WiFi的入侵检测方法及装置

(57)摘要

本发明实施例提供一种基于WiFi的入侵检测方法及装置，包括：根据待检测区域的WiFi信号，获取当前时刻信道状态信息和上一时段信道状态信息；将所述当前时刻信道状态和所述上一时段信道状态信息进行比较，得到信道状态信息的变化量，以用于获取所述待检测区域的入侵状态。本发明实施例通过对待测区域内WiFi信号的信道状态信息的变化量进行分析处理，从而判断待测区域是否存在入侵情况，提高了入侵检测的准确性和灵敏度，并使得入侵检测的范围更加全面。



CN 110012496 A

1.一种基于WiFi的入侵检测方法,其特征在于,包括:

根据待检测区域的WiFi信号,获取当前时刻信道状态信息和上一时段信道状态信息;

将所述当前时刻信道状态和所述上一时段信道状态信息进行比较,得到信道状态信息的变化量,以用于获取所述待检测区域的入侵状态。

2.根据权利要求1所述的基于WiFi的入侵检测方法,其特征在于,所述根据待检测区域的WiFi信号,获取当前时刻信道状态信息和上一时段信道状态信息,包括:

根据待检测区域的WiFi信号,得到所述WiFi信号的信道状态信息;

将所述信道状态信息对应的子载波、天线和接收帧进行排序,得到当前时刻信道状态信息和上一时段信道状态信息。

3.根据权利要求2所述的基于WiFi的入侵检测方法,其特征在于,在所述根据待检测区域的WiFi信号,得到所述WiFi信号的信道状态信息之后,所述方法还包括:

根据最小二乘拟合对所述信道状态信息进行处理,得到处理后的信道状态信息。

4.根据权利要求1所述的基于WiFi的入侵检测方法,其特征在于,所述将所述当前时刻信道状态和所述上一时段信道状态信息进行比较,得到信道状态信息的变化量,以用于获取所述待检测区域的入侵状态,包括:

分别获取第一信道状态和第二信道状态,所述第一信道状态通过所述当前时刻信道状态对应子载波的幅度信息和相位信息得到,所述第二信道状态通过所述上一时段信道状态信息对应子载波的幅度信息和相位信息得到;

将所述第一信道状态与所述第二信道状态进行比较,得到信道状态变化量,并根据所述信道状态变化量的平方和进行判断,以得到所述待检测区域的入侵状态。

5.根据权利要求4所述的基于WiFi的入侵检测方法,其特征在于,所述将所述第一信道状态与所述第二信道状态进行比较,得到信道状态变化量,并根据所述信道状态变化量的平方和进行判断,以得到所述待检测区域的入侵状态,包括:

根据所述第一信道状态与所述第二信道状态的差异值,得到信道状态变化量;

通过预设阈值对所述信道状态变化量的平方和进行判断,所述预设阈值包括预警阈值和入侵阈值,其中,若所述信道状态变化量的平方和大于等于所述入侵阈值,则判断获知所述待检测区域已处于入侵状态。

6.根据权利要求5所述的基于WiFi的入侵检测方法,其特征在于,所述通过预设阈值对所述信道状态变化量的平方和进行判断,还包括:

若所述信道状态变化量的平方和小于所述入侵阈值,且大于所述预警阈值,则判断获知所述待检测区域存在入侵风险;

若所述信道状态变化量的平方和小于所述预警阈值,则判断获知所述待检测区域处于安全状态。

7.一种基于WiFi的入侵检测装置,其特征在于,包括:

信号获取模块,用于根据待检测区域的WiFi信号,获取当前时刻信道状态信息和上一时段信道状态信息;

入侵检测模块,用于将所述当前时刻信道状态和所述上一时段信道状态信息进行比较,得到信道状态信息的变化量,以用于获取所述待检测区域的入侵检测结果。

8.根据权利要求7所述的基于WiFi的入侵检测装置,其特征在于,所述装置还包括:可

视化模块，用于将所述入侵检测模块得到的入侵检测判断结果转换为可视化信息，并将所述可视化信息发送到显示终端进行显示。

9.一种电子设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述处理器执行所述程序时实现如权利要求1至6任一项所述方法的步骤。

10.一种非暂态计算机可读存储介质，其上存储有计算机程序，其特征在于，该计算机程序被处理器执行时实现如权利要求1至6任一项所述方法的步骤。

一种基于WiFi的入侵检测方法及装置

技术领域

[0001] 本发明涉及安防技术领域，尤其涉及一种基于WiFi的入侵检测方法及装置。

背景技术

[0002] 入侵检测技术是一种对周边区域环境中的移动目标进行监测，同时对非法入侵的人员发出警报以及提醒相关人员的检测技术。传统的入侵检测技术都存在一定的缺陷，例如视频监控因摄像头位置存在监测盲区，红外线和超声波等检测方法需要额外进行设备安装，带来较高的硬件成本。

[0003] 随着WiFi技术的不断发展，WiFi技术以其传输速度快、成本低和安装简易等优点，在家庭、办公场所和公共区域得到广泛部署和应用。利用WiFi技术进行入侵检测，可以更加有效的使用现有无线网络基础设施，同时能够解决传统入侵检测方法需要单独设置入侵检测硬件的投入，以及入侵检测设备大部分时间处于闲置状态而导致的资源浪费的问题。

[0004] 目前，现有技术通过MAC层提取接收信号强度(Received Signal Strength Indicator，简称RSSI)信息，以进行入侵检测。然而，由于RSSI信息只含有一个总带宽信号强度，当无线信号在传播时，即使区域内未出现入侵，RSSI信息也会出现剧烈的变化，导致入侵检测的精度低，出现误报等问题。因此，现在亟需一种基于WiFi的入侵检测方法及装置来解决上述问题。

发明内容

[0005] 针对现有技术存在的问题，本发明实施例提供一种基于WiFi的入侵检测方法及装置。

[0006] 第一方面，本发明实施例提供了一种基于WiFi的入侵检测方法，包括：

[0007] 根据待检测区域的WiFi信号，获取当前时刻信道状态信息和上一时段信道状态信息；

[0008] 将所述当前时刻信道状态和所述上一时段信道状态信息进行比较，得到信道状态信息的变化量，以用于获取所述待检测区域的入侵状态。

[0009] 第二方面，本发明实施例提供了一种基于WiFi的入侵检测装置，包括：

[0010] 信号获取模块，用于根据待检测区域的WiFi信号，获取当前时刻信道状态信息和上一时段信道状态信息；

[0011] 入侵检测模块，用于将所述当前时刻信道状态和所述上一时段信道状态信息进行比较，得到信道状态信息的变化量，以用于获取所述待检测区域的入侵检测结果。

[0012] 第三方面，本发明实施例提供一种电子设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现如第一方面所提供的方法的步骤。

[0013] 第四方面，本发明实施例提供一种非暂态计算机可读存储介质，其上存储有计算机程序，该计算机程序被处理器执行时实现如第一方面所提供的方法的步骤。

[0014] 本发明实施例提供的一种基于WiFi的入侵检测方法及装置，通过对待测区域内WiFi信号的信道状态信息的变化量进行分析处理，从而判断待测区域是否存在入侵情况，提高了入侵检测的准确性和灵敏度，并使得入侵检测的范围更加全面。

附图说明

[0015] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0016] 图1为本发明实施例提供的基于WiFi的入侵检测方法的流程示意图；

[0017] 图2为本发明实施例提供的基于WiFi的入侵检测装置的结构示意图；

[0018] 图3为本发明实施例提供的电子设备结构示意图。

具体实施方式

[0019] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0020] 图1为本发明实施例提供的基于WiFi的入侵检测方法的流程示意图，如图1所示，本发明实施例提供了一种基于WiFi的入侵检测方法，包括：

[0021] 步骤101，根据待检测区域的WiFi信号，获取当前时刻信道状态信息和上一时段信道状态信息。

[0022] 在本发明实施例中，首先，在对待测区域的入侵情况进行检测前，需要对待测区域内的WiFi信号进行处理，从WiFi信号中提取信道状态信息(Channel State Information，简称CSI)，CSI中携带有每个子载波的信道频率响应，包含每个子载波的幅度信息和相位信息，这些信息在静态条件下，相比RSSI信息，具有更加稳定的状态。当待测区域内的环境状态发生变化时，例如，由于待测区域内有新的人体或者物体位置发生改变，从而导致CSI中子载波的幅度信息和相位信息发生了变化。在本发明实施例中，通过获取当前时刻CSI和上一时段CSI，判断待测区域是否处于入侵状态，需要说明的是，上一时段CSI可根据实际检测要求进行设置，例如，设置当前时刻前1秒内的CSI或者前一个数据帧作为上一时段CSI，从而根据CSI的幅度信息和相位信息的变化情况来判断入侵状态。进一步地，在本发明一实施例中，在对待检测区域进行入侵判断之前，需要对待检测区域在无人入侵情况下的WiFi信号进行采集，为了消除WiFi信号的相位随机化影响，通过最小二乘拟合或者求取相差的方式对WiFi信号进行去除随机化的处理，从而得到待检测区域在无人入侵情况下稳定的WiFi信号。

[0023] 步骤102，将所述当前时刻信道状态和所述上一时段信道状态信息进行比较，得到信道状态信息的变化量，以用于获取所述待检测区域的入侵状态。

[0024] 在本发明实施例中，在待检测区域内，WiFi信号会经过一系列的反射、衍射和散射，在发射端和接收端之间进行传播，在待测区域内的固定物体保持不变的情况下，CSI中

的幅度信息和相位信息将处于变化规律稳定的状态，需要说明的是，在本发明实施例中，在对CSI进行分析时，将其他电子设备的信号干扰以及硬件差异性等因素也进行了考虑，例如，因WiFi信号发射端处于长时间工作，而导致发射功率下降造成的差异，或者WiFi工作频段存在干扰，通过提前根据硬件属性造成的差异对预设阈值进行设置或者校准，从而对因信号干扰以及硬件差异性造成的CSI变化进行了排除，以提高入侵检测的准确性。进一步地，在本发明实施例中，在获取到当前时刻CSI和上一时段CSI之后，对获取到的数据进行均值或平方和等特性分析，判断在待测区域内，是否存在入侵危险，进一步地，根据CSI的变化情况进行分析，还可以判断入侵目标的行为特征，例如，入侵目标处于移动状态或者静止状态等。

[0025] 本发明实施例提供的一种基于WiFi的入侵检测方法，通过对待测区域内WiFi信号的信道状态信息的变化量进行分析处理，从而判断待测区域是否存在入侵情况，提高了入侵检测的准确性和灵敏度，并使得入侵检测的范围更加全面。

[0026] 在上述实施例的基础上，所述根据待检测区域的WiFi信号，获取当前时刻信道状态信息和上一时段信道状态信息，包括：

[0027] 根据待检测区域的WiFi信号，得到所述WiFi信号的信道状态信息；

[0028] 将所述信道状态信息对应的子载波、天线和接收帧进行排序，得到当前时刻信道状态信息和上一时段信道状态信息。

[0029] 在本发明实施例中，对待检测区域的WiFi信号进行提取，得到对应的CSI，然后，将CSI对应的子载波、天线和接收帧的序号进行排序，即对每一个CSI进行排序，具体地，根据接收端的WiFi设备的天线数量，将天线按顺序进行排序，再将每一根天线接收的子载波按顺序进行排序，最后根据接收帧序号将接收到的CSI进行排序，表示为:H(i,j,k)，分别表示H的频域、空域、时域维度。其中，H表示信道状态信息，i表示子载波序号，j表示天线序号，k表示接收帧序号，例如，H(2,1,5)表示接收端WiFi设备第一根天线接收的第二个子载波第5帧对应的CSI。进一步地，在对每一个CSI进行排序之后，获取同一个天线接收的同一子载波中当前帧的CSI和上一帧的CSI，从而得到当前时刻CSI和上一时段CSI。需要说明的是，在本发明实施例中，获取到的上一时段CSI可以根据实际检测需求进行设置，例如，将当前帧的CSI作为当前时刻CSI，并将当前帧前5帧或者前1帧的CSI作为上一时段CSI。

[0030] 在上述实施例的基础上，在所述根据待检测区域的WiFi信号，得到所述WiFi信号的信道状态信息之后，所述方法还包括：

[0031] 根据最小二乘拟合对所述信道状态信息进行处理，得到处理后的信道状态信息。

[0032] 在本发明实施例中，由于无线信道的随机性，信道状态信息受时间、空间和频率的影响，每个H(i,j,k)都不相同，因此，需要对不同时刻的H的变化规律进行分析。由于CSI中各子载波之间存在一定的相位差，同时CSI存在跨2π的模糊问题，在本发明实施例中，通过最小二乘拟合(Least-square fitting)或者求取天线相差的方式对其进行优化处理，以使得经过优化处理后CSI的时间信息、频率信息和空间信息存在相关性，从而可以表征某个时刻的信道状态，同时，也避免了相位随机性的影响。

[0033] 在上述实施例的基础上，所述将所述当前时刻信道状态和所述上一时段信道状态信息进行比较，得到信道状态信息的变化量，以用于获取所述待检测区域的入侵状态，包括：

[0034] 分别获取第一信道状态和第二信道状态，所述第一信道状态通过所述当前时刻信道状态对应子载波的幅度信息和相位信息得到，所述第二信道状态通过所述上一时段信道状态信息对应子载波的幅度信息和相位信息得到；

[0035] 将所述第一信道状态与所述第二信道状态进行比较，得到信道状态变化量，并根据信道状态变化量的平方和进行判断，以得到所述待检测区域的入侵状态。

[0036] 在本发明实施例中，通过信道状态方差的变化反映CSI的波动情况，并对CSI的波动情况进行分析，当待测区域内有目标入侵时，信道状态变化量将呈现大幅度的变化，即CSI的波动程度将会变大，在排除其他电子设备干扰或者发射端与接收端位置改变的影响下，对CSI的波动情况进行分析，从而判断待检测区域的入侵状态。具体地，在本发明实施例中，相位差的获取方法，可以直接通过两个CSI复数共轭乘获取，相位差公式如下：

[0037] (CSI_I[l]+j×CSI_Q[l])×Conjugate(CSI_I[m]+j×CSI_Q[m])；

[0038] 其中，l和m表示CSI索引，可以为子载波天线和帧的任一维度，CSI_I和CSI_Q分别表示CSI复数的实数部分和虚数部分，Conjugate表示求取共轭的操作。

[0039] 需要说明的是，在本发明实施例中，优选地，通过对多个帧、多个天线和多个子载波变化量的平方和共同作用进行判断，可进一步提高入侵检测的成功率，从而降低入侵检测误报率。

[0040] 在上述实施例的基础上，所述将所述第一信道状态与所述第二信道状态进行比较，得到信道状态变化量，并根据所述信道状态变化量的平方和进行判断，以得到所述待检测区域的入侵状态，包括：

[0041] 根据所述第一信道状态与所述第二信道状态的差异性，得到信道状态变化量；

[0042] 通过预设阈值对所述信道状态变化量的平方和进行判断，所述预设阈值包括预警阈值和入侵阈值，其中，若所述信道状态变化量的平方和大于等于所述入侵阈值，则判断获知所述待检测区域已处于入侵状态。

[0043] 在本发明实施例中，通过将第一信道状态和第二信道状态的幅度、相位或者相差进行比较，根据比较得到的差异性，获取信道状态变化量。需要说明的是，在本发明实施例中，预设阈值可根据信道干扰情况和接收信号功率进行调整；另外，为了避免接收信号功率本身对入侵判断的影响，还可以通过接收信号功率对信道状态变化量的平方和进行归一化处理。

[0044] 在上述实施例的基础上，所述通过预设阈值对所述信道状态变化量的平方和进行判断，还包括：

[0045] 若所述信道状态变化量的平方和小于所述入侵阈值，且大于所述预警阈值，则判断获知所述待检测区域存在入侵风险；

[0046] 若所述信道状态变化量的平方和小于所述预警阈值，则判断获知所述待检测区域处于安全状态。

[0047] 在本发明实施例中，WiFi信号在传播的过程中，若遇到障碍物，便会产生反射、衍射和散射等现象，特别当WiFi信号穿过人体时，部分信号可能发生散射和反射等现象，部分信号可能会被人体吸收，因此，当WiFi信号传播链路之间有人体穿过时，WiFi信号会发生较大程度的波动，即通过WiFi信号中的CSI在受到人体干扰时呈现的不同变化，从而进行入侵检测。在本发明实施例中，在对信道状态变化量的平方和进行分析之前，还可以对CSI进行

数据预处理，通过进行数据异常点清理，从而减少外界噪声对CSI产生的影响。然后对得到的信道状态变化量的平方和进行分析，需要说明的是，在本发明实施例中，可通过支持向量机或神经网络建立入侵检测模型对信道状态变化量的平方和进行入侵判断分析，具体的模型构建方式在本发明实施例中不作限定。

[0048] 进一步地，在对信道状态变化量进行分析时，根据信道状态变化量的平方和和预设阈值之间的对比，得到对应的入侵情况判断，在一个本发明的实施例中，通过在待测区域内，例如酒店房间、银行金库或家庭住宅内，在这些区域内墙角或者墙边各设置一个WiFi设备，这些WiFi设备形成了WiFi无线通路，由于多次直射、反射和衍射，使得无线信号分布在整个区域内，因此，区域内无线信号的任何扰动，都会导致接收端接收到的无线信号发生变化，即CSI也会发生相应的变化。然后，对任一WiFi设备接收的WiFi信号进行CSI提取，在本发明一实施例中，提取CSI的设备可以为无线AP(AccessPoint，简称AP)设备。AP完成检测处理后通过与无线AP设备相连接的网络(有线网络或者无线网状网络)将信号发送到监测中心或者移动监测终端；在本发明另一实施例中，提取CSI的设备可以为终端站点(Station，简称STA)设备，此时STA设备可以将入侵检测结果传输给AP设备，AP设备再将入侵检测结果进一步发送给监测中心或者通过网络发送给移动监测终端或者手机APP。

[0049] 优选地，在本发明实施例中，将用于判断入侵状态的预设阈值设置为入侵阈值和预警阈值，从而可以更加精准的判断入侵的程度，并将入侵状态发送到监测终端，以使得监测人员根据入侵状态进行相应的应对措施。具体地，根据检测区域的复杂程度对预设阈值进行相应的设置，并且入侵阈值大于预警阈值，以使得入侵阈值和预警阈值构成一个阈值范围，从而对落入对应范围内的信道状态变化量的平方和进行判断，例如，当待测区域内的信道状态变化量的平方和大于等于入侵阈值时，可以判断得知在该区域内有人入侵，并根据一系列信道状态变化量的平方和的大小，结合支持向量机或者神经网络，判断入侵者的活动行为，例如，开门行为、站立或者静止等动作；当待测区域内的信道状态变化量的平方和小于入侵阈值，且大于预警阈值时，此时在待测区域内可能并未有人为行动造成的入侵，其出现人为入侵的可能性随信道状态变化量的平方和的大小判断，越接近入侵阈值，则越有可能属于人为入侵，例如，当被检测区域为家庭住宅时，可能出现宠物进入被测区域的情况，或者窗户未关造成的物件被吹散的情况，此时信道状态变化量的平方和大于预警阈值，但远小于入侵阈值，相关人员根据这些信息，可以采取相应的措施。

[0050] 图2为本发明实施例提供的基于WiFi的入侵检测装置的结构示意图，如图2所示，本发明实施例提供了一种基于WiFi的入侵检测装置，包括：信号获取模块201和入侵检测模块202，其中，信号获取模块201用于根据待检测区域的WiFi信号，获取当前时刻信道状态信息和上一时段信道状态信息；入侵检测模块202用于将所述当前时刻信道状态和所述上一时段信道状态信息进行比较，得到信道状态信息的变化量，以用于获取所述待检测区域的入侵检测结果。

[0051] 在本发明实施例中，首先，入侵检测模块202在对待测区域的入侵情况进行检测前，信号获取模块201需要对待测区域内的WiFi信号进行处理，从WiFi信号中CSI，CSI中携带有每个子载波的信道频率响应，包含每个子载波的幅度信息和相位信息，在待测区域内有新的人体或者物体位置发生改变，将会导致CSI中子载波的幅度信息和相位信息发送了变化。在本发明实施例中，信号获取模块201获取当前时刻CSI和上一时段CSI，以供入侵检

测模块202判断待测区域是否处于入侵状态，需要说明的是，上一时段CSI可根据实际检测要求进行设置，例如，设置当前时刻前1秒或者1个数据帧内的CSI作为上一时段CSI，从而根据CSI的幅度信息和相位信息的变化情况来判断入侵状态。

[0052] 本发明实施例提供的一种基于WiFi的入侵检测装置，通过对待测区域内WiFi信号的信道状态信息的变化量进行分析处理，从而判断待测区域是否存在入侵情况，提高了入侵检测的准确性和灵敏度，并使得入侵检测的范围更加全面。

[0053] 在上述实施例的基础上，所述信号获取模块201包括：信道状态信息提取单元和信道状态信息排序单元，其中，信道状态信息提取单元用于根据待检测区域的WiFi信号，得到所述WiFi信号的信道状态信息；信道状态信息排序单元用于将所述信道状态信息对应的子载波、天线和接收帧进行排序，得到当前时刻信道状态信息和上一时段信道状态信息。

[0054] 在上述实施例的基础上，所述装置还包括：优化处理模块，用于根据最小二乘拟合对所述信道状态信息进行处理，得到处理后的信道状态信息。

[0055] 在上述实施例的基础上，所述入侵检测模块202包括：处理单元和入侵检测判断单元，其中，处理单元用于分别获取第一信道状态和第二信道状态，所述第一信道状态通过所述当前时刻信道状态对应子载波的幅度信息和相位信息得到，所述第二信道状态通过所述上一时段信道状态信息对应子载波的幅度信息和相位信息得到；入侵检测判断单元用于将所述第一信道状态与所述第二信道状态进行比较，得到信道状态变化量，并根据所述信道状态变化量的平方和进行判断，以得到所述待检测区域的入侵状态。

[0056] 在上述实施例的基础上，所述入侵检测判断单元包括：变化量获取子单元和第一入侵状态判断子单元，其中，变化量获取子单元用于根据所述第一信道状态与所述第二信道状态的差异值，得到信道状态变化量；第一入侵状态判断子单元用于通过预设阈值对所述信道状态变化量的平方和进行判断，所述预设阈值包括预警阈值和入侵阈值，其中，若所述信道状态变化量的平方和大于等于所述入侵阈值，则判断获知所述待检测区域已处于入侵状态。

[0057] 在上述实施例的基础上，所述入侵状态判断子单元还包括：第二入侵状态判断子单元和第三入侵状态判断子单元，其中，第二入侵状态判断子单元用于若所述信道状态变化量的平方和小于所述入侵阈值，且大于所述预警阈值，则判断获知所述待检测区域存在入侵风险；第三入侵状态判断子单元用于若所述信道状态变化量的平方和小于所述预警阈值，则判断获知所述待检测区域处于安全状态。其中，在一般情况下，入侵阈值大于预警阈值；在特定情况下，预警阈值可设置为与入侵阈值一致。

[0058] 在上述实施例的基础上，所述装置还包括：可视化模块，用于将所述入侵检测模块202得到的入侵检测判断结果转换为可视化信息，并将所述可视化信息发送到显示终端进行显示。

[0059] 在本发明实施例中，可视化模块用于将入侵检测模块202得到的检测结果转换为可视化信息，然后通过网络将信息发送到显示终端进行显示，例如监控中心或者手机APP，操作人员在收到信息后可以采取相应的应对措施。在本发明实施例中，操作人员接收到的可视化信息除了图像信息，还可以是声音信息或者电信息，直接通过语音提示的方式、警示灯方式或者振动手环方式等，将当前入侵状态告知操作人员。

[0060] 本发明实施例提供的基于WiFi的入侵检测装置，通过对现有WiFi设备的信号进行

检测分析,在检测过程中,不影响现有WiFi设备的自适应调制与编码策略(Modulation and Coding Scheme,简称MCS)、功率控制和业务传输等功能,并且检测设备具有正常的通讯设备功能,从而实现节省设备的监控检测。

[0061] 本发明实施例提供的装置是用于执行上述各方法实施例的,具体流程和详细内容请参照上述实施例,此处不再赘述。

[0062] 图3为本发明实施例提供的电子设备结构示意图,如图3所示,该电子设备可以包括:处理器(Processor)301、通信接口(Communications Interface)302、存储器(Memory)303和通信总线304,其中,处理器301,通信接口302,存储器303通过通信总线304完成相互间的通信。处理器301可以调用存储器303中的逻辑指令,以执行如下方法:根据待检测区域的WiFi信号,获取当前时刻信道状态信息和上一时段信道状态信息;将所述当前时刻信道状态和所述上一时段信道状态信息进行比较,得到信道状态信息的变化量,以用于获取所述待检测区域的入侵状态。

[0063] 此外,上述的存储器303中的逻辑指令可以通过软件功能单元的形式实现并作为独立的产品销售或使用时,可以存储在一个计算机可读取存储介质中。基于这样的理解,本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质中,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备等)执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括:U盘、移动硬盘、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0064] 本发明实施例公开一种计算机程序产品,所述计算机程序产品包括存储在非暂态计算机可读存储介质上的计算机程序,所述计算机程序包括程序指令,当所述程序指令被计算机执行时,计算机能够执行上述各方法实施例所提供的方法,例如包括:根据待检测区域的WiFi信号,获取当前时刻信道状态信息和上一时段信道状态信息;将所述当前时刻信道状态和所述上一时段信道状态信息进行比较,得到信道状态信息的变化量,以用于获取所述待检测区域的入侵状态。

[0065] 本发明实施例提供一种非暂态计算机可读存储介质,该非暂态计算机可读存储介质存储服务器指令,该计算机指令使计算机执行上述实施例所提供的基于WiFi的入侵检测方法,例如包括:根据待检测区域的WiFi信号,获取当前时刻信道状态信息和上一时段信道状态信息;将所述当前时刻信道状态和所述上一时段信道状态信息进行比较,得到信道状态信息的变化量,以用于获取所述待检测区域的入侵状态。

[0066] 最后应说明的是:以上实施例仅用以说明本发明的技术方案,而非对其限制;尽管参照前述实施例对本发明进行了详细的说明,本领域的普通技术人员应当理解:其依然可以对前述各实施例所记载的技术方案进行修改,或者对其中部分技术特征进行等同替换;而这些修改或者替换,并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

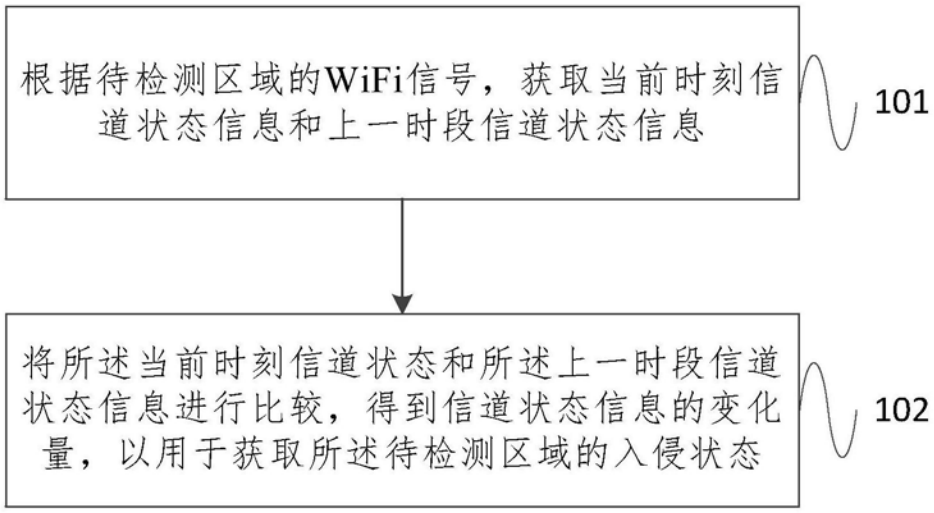

根据待检测区域的WiFi信号，获取当前时刻信道状态信息和上一时段信道状态信息
101
将所述当前时刻信道状态和所述上一时段信道状态信息进行比较，得到信道状态信息的变化量，以用于获取所述待检测区域的入侵状态
102

图1

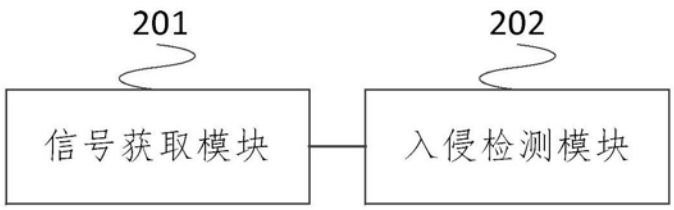

201
202
信号获取模块
入侵检测模块

图2

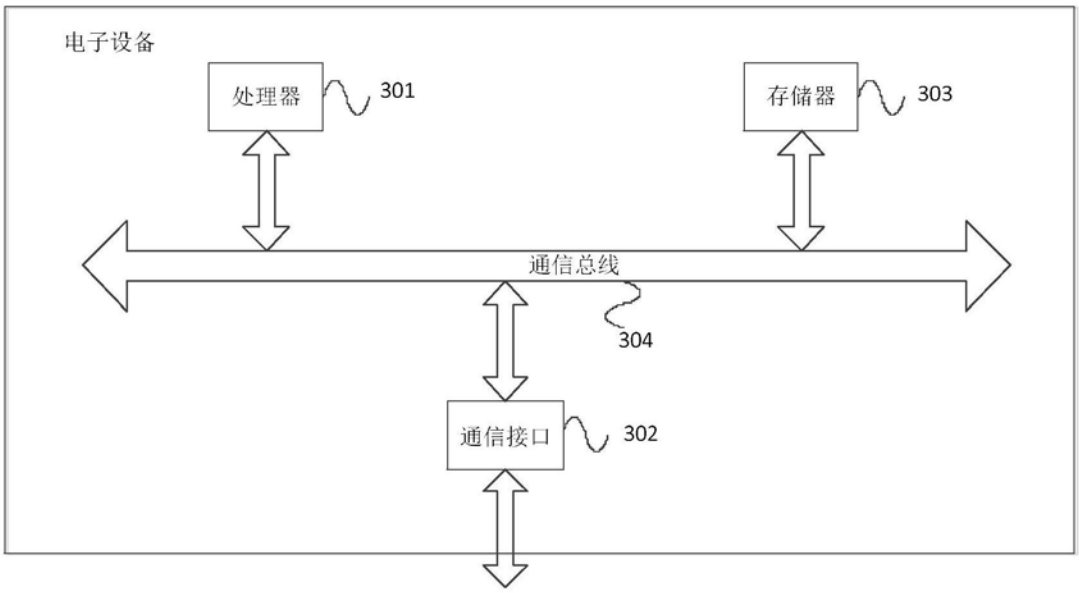

电子设备
处理器
301
存储器
303
通信总线
304
通信接口
302

图3